

**HUNTON ANDREWS KURTH LLP**

Ann Marie Mortimer (State Bar No. 169077)

amortimer@HuntonAK.com

Jason J. Kim (State Bar No. 221476)

kimj@HuntonAK.com

Jeff R. R. Nelson (State Bar No. 301546)

jnelson@HuntonAK.com

550 South Hope Street, Suite 2000

Los Angeles, California 90071-2627

Telephone: (213) 532-2000

Facsimile: (213) 532-2020

Attorneys for Defendant

WALMART INC.

**UNITED STATES DISTRICT COURT  
NORTHERN DISTRICT OF CALIFORNIA  
OAKLAND DIVISION**

LAVARIOUS GARDINER, individually  
and on behalf of all others similarly  
situated,

Plaintiff,

v.

WALMART INC., et al.,

Defendants.

CASE NO.: 4:20-cv-04618-JSW

**DEFENDANT WALMART INC.'S  
NOTICE OF MOTION AND MOTION  
TO DISMISS PLAINTIFF'S  
COMPLAINT**

[Request for Judicial Notice filed  
concurrently herewith]

Date: March 5, 2021

Time: 9:00 a.m.

Location: Ctrm. 5

Hunton Andrews Kurth LLP  
 550 South Hope Street, Suite 2000  
 Los Angeles, California 90071-2627

**TO PLAINTIFF AND HIS ATTORNEYS OF RECORD:**

PLEASE TAKE NOTICE that, on March 5, 2021 at 9:00 a.m., or as soon thereafter as the matter may be heard in Courtroom 5 of the above-entitled Court located at 1301 Clay Street, Oakland, California, Defendant Walmart Inc. (“Walmart”) will move this Court for an order dismissing this lawsuit in its entirety.

This motion is made on the grounds that Plaintiff has not stated viable claims. *First*, Plaintiff fails to allege *when* the alleged breach at issue (the “Alleged Breach”) occurred, which controls whether the California Consumer Privacy Act (“CCPA”) even applies. Plaintiff also fails to allege “personal information” was compromised. Cal. Civ. Code § 1798.81.5(d)(1)(a). *Second*, Plaintiff fails to allege cognizable injury with respect to his remaining claims (negligence, unfair competition (“UCL”), and his contract theories). *Third*, Plaintiff’s negligence claim fails under the economic loss rule because he cannot allege personal injury or property damage. *Fourth*, Plaintiff’s UCL claim fails because he cannot show: (1) he lacks adequate legal remedies (*Sonner v. Premier Nutrition Corp.*, 971 F.3d 834, 845 (9th Cir. 2020)); or (2) any predicate “unlawful,” “fraudulent,” or “unfair” conduct. *Fifth*, Plaintiff’s contract claims are barred by the limitation-of-liability provision in Walmart’s Terms of Use.

This motion is based upon this Notice of Motion and Motion, the attached Memorandum of Points and Authorities, the Request for Judicial Notice filed concurrently herewith, all the pleadings and papers on file herein, and on such other evidence and argument as may be presented at the hearing on this matter.

Dated: December 14, 2020

**HUNTON ANDREWS KURTH LLP**

By: /s/ Ann Marie Mortimer

Ann Marie Mortimer

Jason J. Kim

Jeff R. R. Nelson

Attorneys for Defendant

WALMART INC.

**TABLE OF CONTENTS**

I. INTRODUCTION ..... 1

II. STATEMENT OF ISSUES TO BE DECIDED..... 2

III. FACTS..... 2

IV. PLAINTIFF’S PLEADING BURDEN ..... 3

V. PLAINTIFF FAILS TO STATE VIABLE CLAIMS FOR RELIEF..... 4

    A. Plaintiff’s CCPA Claim Fails (Count I)..... 4

    B. Plaintiff Fails to Allege the Requisite Injuries With Respect to His  
        Remaining Claims ..... 6

    C. Plaintiff’s Claims Fail for Additional Reasons ..... 10

        1. Plaintiff’s Negligence Claim Fails (Count II) ..... 10

        2. Plaintiff’s Unfair Competition Claim Fails (Count III)..... 10

        3. Plaintiff’s Contract Theories Fail (Counts IV-VI) ..... 13

VI. CONCLUSION ..... 15

Hunton Andrews Kurth LLP  
550 South Hope Street, Suite 2000  
Los Angeles, California 90071-2627

**TABLE OF AUTHORITIES****Page(s)****Cases**

<i>Ables v. Brooks Bros. Grp.</i> , 2018 WL 8806667 (C.D. Cal. June 7, 2018).....	6, 7, 9, 10
<i>Adams v. Cole Haan, LLC</i> , 2020 WL 5648605 (C.D. Cal. Sept. 3, 2020).....	11
<i>Adams v. Johnson</i> , 355 F.3d 1179 (9th Cir. 2004) .....	3
<i>In re Adobe Sys., Inc. Privacy Litig.</i> , 66 F. Supp. 3d 1197 (N.D. Cal. 2014).....	6
<i>Aetna Cas. &amp; Sur. Co. v. Indus. Acci. Com.</i> , 30 Cal. 2d 388 (1947) .....	4
<i>Aguilera v. Pirelli Armstrong Tire Corp.</i> , 223 F.3d 1010 (9th Cir. 2000) .....	6
<i>Ashcroft v. Iqbal</i> , 556 U.S. 662 (2009).....	3
<i>Baba v. Hewlett-Packard Co.</i> , 2010 WL 2486353 (N.D. Cal. June 16, 2010).....	13
<i>Beck v. McDonald</i> , 848 F.3d 262 (4th Cir. 2017) .....	7
<i>Bell Atlantic Corp. v. Twombly</i> , 550 U.S. 544 (2007).....	3
<i>Californians for Disability Rights v. Mervyn's, LLC</i> , 39 Cal. 4th 223 (2006) .....	4
<i>Caraccioli v. Facebook, Inc.</i> , 167 F. Supp. 3d 1056 (N.D. Cal. 2016).....	15
<i>Castillo v. Seagate Tech., LLC</i> , 2016 WL 9280242 (N.D. Cal. Sept. 14, 2016).....	10

1	<i>Cel-Tech Commc'ns, Inc. v. Los Angeles Cellular Tel. Co.,</i>	
2	20 Cal. 4th 163 (1999).....	12
3	<i>Dugas v. Starwood Hotels &amp; Resorts Worldwide, Inc.,</i>	
4	2016 WL 6523428 (S.D. Cal. Nov. 3, 2016).....	11, 12
5	<i>Engl v. Nat. Grocers by Vitamin Cottage, Inc.,</i>	
6	2016 WL 8578252 (D. Colo. Sept. 21, 2016) .....	9
7	<i>Erickson v. Neb. Mach. Co.,</i>	
8	2015 WL 4089849 (N.D. Cal. July 6, 2015) .....	8
9	<i>Evangelatos v. Superior Court,</i>	
10	44 Cal. 3d 1188 (1988).....	4
11	<i>In re Facebook Privacy Litig.,</i>	
12	791 F. Supp. 2d 705 (N.D. Cal. 2011).....	12
13	<i>Fonseca v. Goya Foods, Inc.,</i>	
14	2016 WL 4698942 (N.D. Cal. Sept. 8, 2016).....	11
15	<i>Food Safety Net Servs. v. Eco Safe Sys. USA, Inc.,</i>	
16	209 Cal. App. 4th 1118 (2012).....	14, 15
17	<i>Gibson v. Jaguar Land Rover N. Am., LLC,</i>	
18	2020 WL 5492990 (C.D. Cal. Sept. 9, 2020).....	10
19	<i>In re Google Inc. St. View Elec. Commc'ns Litig.,</i>	
20	794 F. Supp. 2d 1067 (N.D. Cal. 2011).....	12
21	<i>In re iPhone Application Litig.,</i>	
22	2011 WL 4403963 (N.D. Cal. Sept. 20, 2011).....	12
23	<i>Jackson v. Loews Hotels, Inc.,</i>	
24	2019 WL 2619656 (C.D. Cal. Jan. 4, 2019).....	9
25	<i>Jackson v. Loews Hotels, Inc.,</i>	
26	2019 WL 6721637 (C.D. Cal. July 24, 2019) .....	8
27	<i>Khan v. Children's Nat'l Health Sys.,</i>	
28	188 F. Supp. 3d 524 (D. Md. 2016).....	8
	<i>In re Macbook Keyboard Litig.,</i>	
	2020 WL 6047253 (N.D. Cal. Oct. 13, 2020) .....	10

1	<i>Madrigal v. Hint, Inc.</i> ,	
2	2017 WL 6940534 (C.D. Cal. Dec. 14, 2017).....	11
3	<i>McClung v. Emp’t Dev. Dep’t</i> ,	
4	34 Cal. 4th 467 (2004).....	4
5	<i>Myers v. Philip Morris Cos., Inc.</i> ,	
6	28 Cal. 4th 828 (2002).....	4
7	<i>Provost v. Aptos, Inc.</i> ,	
8	2018 WL 1465766 (N.D. Ga. Mar. 12, 2018).....	9
9	<i>Rose v. Bank of Am., N.A.</i> ,	
10	57 Cal. 4th 390 (2013).....	12
11	<i>Ruiz v. Gap, Inc.</i> ,	
12	380 F. App’x 689 (9th Cir. 2010).....	6
13	<i>Schertz v. Ford Motor Co.</i> ,	
14	2020 WL 5919731 (C.D. Cal. July 27, 2020) .....	11
15	<i>Smith v. Sabre Corp.</i> ,	
16	No. 17-cv-5149 (C.D. Cal. Jan. 23, 2018).....	8, 9
17	<i>Sonner v. Premier Nutrition Corp.</i> ,	
18	971 F.3d 834 (9th Cir. 2020) .....	1, 10
19	<i>In re Sony Gaming Networks &amp; Customer Data Sec. Breach Litig.</i> ,	
20	903 F. Supp. 2d 942 (S.D. Cal. 2012) .....	10, 12
21	<i>In re Sony Gaming Networks &amp; Customer Data Sec. Breach Litig.</i> ,	
22	996 F. Supp. 2d 942 (S.D. Cal. 2014) .....	7
23	<i>Tobinick v. Novella</i> ,	
24	2015 WL 1526196 (S.D. Fla. Apr. 2, 2015).....	8
25	<i>U.S. v. Security Industrial Bank</i> ,	
26	459 U.S. 70 (1982).....	4
27	<i>Whalen v. Michaels Stores Inc.</i> ,	
28	153 F. Supp. 3d 577 (E.D.N.Y. 2015).....	9
	<i>Whalen v. Michaels Stores, Inc.</i> ,	
	2017 WL 1556116 (2d Cir. May 2, 2017).....	9

*In re Yahoo! Inc. Customer Data Sec. Breach Litig.*,  
2017 WL 3727318 (N.D. Cal. Aug. 30, 2017)..... 5

**Statutes**

Cal. Bus. & Prof. Code § 17204 ..... 2, 6, 11

Cal. Civ. Code § 3..... 4

Cal. Civ. Code § 1798.81.5..... 5, 6

Cal. Civ. Code § 1798.150..... 5, 12, 13

Cal. Civ. Code § 1798.198..... 4

Hunton Andrews Kurth LLP  
550 South Hope Street, Suite 2000  
Los Angeles, California 90071-2627

## MEMORANDUM OF POINTS AND AUTHORITIES

### I. INTRODUCTION

This is not the typical data breach lawsuit in which the defendant publicly admits its computer network has been compromised, with the inevitable follow-on lawsuits. Rather, Plaintiff Lavarious Gardner has taken the highly unusual step of filing this action against Walmart Inc. (“Walmart”) *on the mere suspicion* that Walmart’s computer network has been breached (the “Alleged Breach”). Indeed, Plaintiff bases his claims on the fact that he allegedly found his credentials on the “dark web,” and that he possesses communications with unknown “hackers” who allegedly assured him they were selling “real accounts that belong to Walmart.” Compl. ¶¶ 15-16. In fact, there was no breach of Walmart’s computer network. And Plaintiff’s own allegations seemingly acknowledge the likely possibility that he and other putative class members’ computers—not Walmart’s systems—were compromised. *Id.* ¶ 14 (claiming “hackers obtain access to Walmart accounts by hacking ... Walmart’s customers’ computers.”) (emphasis added). Not surprisingly, Plaintiff’s claims find no basis in law or fact, and each of them should be dismissed with prejudice:

*First*, Plaintiff fails to allege *when* the Alleged Breach supposedly occurred, which is critical to determining whether the CCPA, which went into effect in 2020, even applies. On top of that, Plaintiff fails to allege the compromise of actionable “personal information.”

*Second*, Plaintiff fails to allege cognizable injury and damages with respect to his remaining claims for negligence (Count II) and alleged UCL violations (Count III), as well as his contract theories (Counts IV through VI).

*Third*, Plaintiff’s negligence claim begins and ends with the economic loss rule, as Plaintiff has not and cannot allege personal injury or property damage.

*Fourth*, Plaintiff’s UCL claim fails under recent Ninth Circuit precedent, as he has not and cannot show he lacks adequate legal remedies. *Sonner v. Premier*



*Nutrition Corp.*, 971 F.3d 834, 845 (9th Cir. 2020) (affirming dismissal of UCL claim where the plaintiff “fail[ed] to demonstrate that she lacks an adequate legal remedy”). Similarly, as stated above, Plaintiff fails to allege the requisite injury in fact. *See* Cal. Bus. & Prof. Code 17204. Nor does Plaintiff allege any predicate “unlawful,” “fraudulent,” or “unfair” conduct.

*Finally*, Plaintiff’s contract claims are barred by the limitation-of-liability provision in Walmart’s Terms of Use (“TOU”), which Plaintiff cannot escape.

## **II. STATEMENT OF ISSUES TO BE DECIDED**

Whether Plaintiff’s claims should be dismissed in their entirety and with prejudice based on his failure to state viable claims for relief.

## **III. FACTS**

Plaintiff alleges he gave certain information to Walmart in order to create an online Walmart account—in particular, his “full name[], address[], financial account information, credit card information, and other [unspecified] private identifiable information.” Compl. ¶¶ 3, 7. Plaintiff does not specify when or how many times he did so. Nonetheless, Plaintiff claims, on information and belief, that “his PII was accessed by hackers as a direct result of the [Alleged Breach] that took place at Walmart.” *Id.* ¶ 7.

More notable, however, is what Plaintiff does not allege. Plaintiff does *not* allege when the Alleged Breach occurred. Similarly, Plaintiff does *not* allege any acknowledgment on the part of Walmart that the Alleged Breach occurred; in fact, it did not. So instead, Plaintiff speculates that the Alleged Breach must have occurred because, like most individuals in a modern and digitally connected society, his information allegedly appeared on the dark web. Compl. ¶ 15. Plaintiff also claims the Alleged Breach occurred based on “communications with the hackers in which they state that the accounts they are selling are real accounts that belong to Walmart customers.” *Id.* ¶ 16. Of course, Plaintiff does not claim the supposed “hackers” confirmed the Alleged Breach or otherwise told Plaintiff *how* they allegedly obtained

1 “real accounts that belong to Walmart customers” or whether the source of the alleged  
2 accounts was Walmart or some other breach. *Id.*

3 Plaintiff’s own allegations, however, may fill in that gap. With respect to some  
4 or all of the supposedly compromised Walmart accounts, including his own, Plaintiff  
5 remarkably concedes that the “hackers obtain access to Walmart accounts by hacking  
6 Walmart’s website *and Walmart’s customers’ computers.*” Compl. ¶ 14 (emphasis  
7 added). So Plaintiff acknowledges his alleged issues may have been—and as to many  
8 putative class members in fact were—the product of compromises of customers’ own  
9 computers.

#### 10 **IV. PLAINTIFF’S PLEADING BURDEN**

11 To survive dismissal, plaintiffs must allege facts that demonstrate a “plausible”  
12 basis for relief. *Bell Atlantic Corp. v. Twombly*, 550 U.S. 544, 556 (2007).

13 “Threadbare recitals of the elements of a cause of action, supported by mere  
14 conclusory statements, do not suffice.” *Ashcroft v. Iqbal*, 556 U.S. 662, 678 (2009).  
15 Indeed, the complaint must “raise a reasonable expectation that discovery will reveal  
16 evidence of [the alleged infraction].” *Twombly*, 550 U.S. at 556. “[A] plaintiff’s  
17 obligation to provide the ‘grounds’ of his ‘entitle[ment] to relief’ requires more than  
18 labels and conclusions, and a formulaic recitation of the elements of a cause of action  
19 will not do.” *Id.* at 555. A plaintiff must plead “factual content that allows the court  
20 to draw the reasonable inference that the defendant is liable for the misconduct  
21 alleged.” *Iqbal*, 556 U.S. at 678. A claim is “plausible” only when the factual  
22 allegations allow the court “to draw the reasonable inference that the defendant is  
23 liable for the misconduct alleged.” *Id.* Factual allegations that establish no “more  
24 than a sheer possibility” of liability are not sufficient. *Id.* Indeed, mere “conclusory  
25 allegations of law and unwarranted inferences are insufficient to defeat a motion to  
26 dismiss.” *Adams v. Johnson*, 355 F.3d 1179, 1183 (9th Cir. 2004).

**V. PLAINTIFF FAILS TO STATE VIABLE CLAIMS FOR RELIEF**

**A. Plaintiff's CCPA Claim Fails (Count I)**

Even assuming the Alleged Breach occurred, which it did not, Plaintiff fails to allege facts showing the CCPA even applies.

*First*, Plaintiff fails to allege *when* the Alleged Breach occurred. This omission is fatal because the CCPA applies only to data breaches that occurred after January 1, 2020, and it cannot be applied retroactively.

“Generally, statutes operate prospectively only.” *McClung v. Emp’t Dev. Dep’t*, 34 Cal. 4th 467, 475 (2004) (quotations omitted); *see also Evangelatos v. Superior Court*, 44 Cal. 3d 1188, 1209 (1988) (the “first rule of [statutory] construction is that legislation must be considered to the future, not the past...”) (quoting *U.S. v. Security Industrial Bank*, 459 U.S. 70, 78-79 (1982)). This “strong” (*McClung*, 34 Cal. 4th at 475) and “time-honored presumption against retroactive application of statute” may be overcome only if the statute “contains express language of retroactivity or if other sources provide a clear and unavoidable implication that the Legislature intended retroactive application.” *Myers v. Philip Morris Cos., Inc.*, 28 Cal. 4th 828, 843-44 (2002); *see also* Cal. Civ. Code § 3 (“No part of [the California Civil Code] is retroactive, unless expressly so declared”).<sup>1</sup>

The CCPA expressly provides that it is not operative until January 1, 2020, and it contains no express language establishing that it applies retroactively. Cal. Civ. Code § 1798.198(a). Accordingly, the CCPA cannot be applied to data breaches that occurred before January 1, 2020.

<sup>1</sup> “A retrospective law is one which affects rights, obligations, acts, transactions and conditions which are performed or exist prior to the adoption of the statute.” *Aetna Cas. & Sur. Co. v. Indus. Acci. Com.*, 30 Cal. 2d 388, 391 (1947); *see also Californians for Disability Rights v. Mervyn’s, LLC*, 39 Cal. 4th 223, 232 (2006) (a retroactive law “change[s] the legal consequences of past conduct by imposing new or different liabilities based on such conduct”).

Plaintiff cannot avoid dismissal by failing to allege when the Alleged Breach occurred. In *In re Yahoo! Inc. Customer Data Sec. Breach Litig.*, 2017 WL 3727318, at \*38 (N.D. Cal. Aug. 30, 2017), Judge Koh reached this exact conclusion, dismissing a claim under the recently amended California Customer Records Act (“CRA”) where the plaintiffs failed to allege when the alleged violation occurred: “Because the CCAC does not allege when Defendants discovered the 2013 Breach, the Court cannot determine which version of the CRA was in effect at the time that Defendants allegedly violated the CRA.” *Id.* The same reasoning applies here, and the result should be the same. The CCPA claim should be dismissed.<sup>2</sup>

*Second*, Plaintiff fails to allege facts showing the Alleged Breach involved actionable “personal information.” To be actionable under the CCPA, a data breach must result in the disclosure of an individual’s first name or initial and last name in conjunction with the individual’s (1) Social Security number, (2) driver’s license or other government-issued identification number, (3) account number or credit or debit card number, *in combination with any required security code, access code, or password that would permit access to an individual’s financial account*, (4) medical information, (5) health insurance information, or (6) unique biometric identifier. Cal. Civ. Code §§ 1798.150(a)(1), 1798.81.5(d)(1)(a).<sup>3</sup>

<sup>2</sup> Plaintiff’s alleged “evidence” in opposition to Walmart’s motion to compel likely explains why Plaintiff did not plead the date of the Alleged Breach. Plaintiff’s purported cybersecurity expert attached a screenshot to his declaration showing Plaintiff’s alleged information was “checked” on August 10, 2019, well before the CCPA’s January 1, 2020 effective date. ECF No. 27-3 (Easttom Decl.), Exh. 2.

<sup>3</sup> Under the CCPA, “personal information” is “defined in subparagraph (A) of paragraph (1) of subdivision (d) of Section 1798.81.5.” Cal. Civ. Code § 1798.150(a)(1). Section 1798.81.5, in turn, defines “personal information” as “an individual’s first name or first initial and the individual’s last name in combination with” an “[a]ccount number or credit or debit card number, *in combination with any required security code, access code, or password that would permit access to an individual’s financial account.*” (Emphasis added.)

1 While Plaintiff makes vague and generalized references to “financial  
2 information,” he does not allege the specific disclosure of his “account number or  
3 credit or debit card number, *in combination with a password that would permit access*  
4 *to the account.*” Cal. Civ. Code § 1798.81.5(d)(1)(a)(3). The complaint makes no  
5 mention of any compromised “security code, access code, or password” that enabled  
6 hackers to access his bank account(s). Plaintiff’s CCPA claim, therefore, fails under  
7 the plain language of the statute. It should be dismissed.

8 **B. Plaintiff Fails to Allege the Requisite Injuries With Respect to His**  
9 **Remaining Claims**

10 Each of Plaintiff’s remaining claims requires appreciable, non-speculative  
11 injury or damages caused by the defendant’s conduct. *See Ruiz v. Gap, Inc.*, 380 F.  
12 App’x 689, 691 (9th Cir. 2010) (negligence); Cal. Bus. & Prof. Code § 17204 (UCL);  
13 *Aguilera v. Pirelli Armstrong Tire Corp.*, 223 F.3d 1010, 1015 (9th Cir. 2000)  
14 (contract). Plaintiff cannot make the requisite showing of cognizable harm.

15 For example, Plaintiff claims hackers accessed his “financial account  
16 information” and “credit card information.” Compl. ¶ 3. Plaintiff, however, does not  
17 claim any fraudulent charges were made on his card(s)—much less non-reimbursed  
18 ones. *Id.* In fact, Plaintiff alleges no identity theft or fraud whatsoever. Without  
19 specific allegations of actual loss, Plaintiff’s claims fail.

20 Similarly, Plaintiff claims his full name and address were exposed in the  
21 Alleged Breach. Compl. ¶ 3. But Plaintiff does not identify any resulting injuries.  
22 Nor could Plaintiff plausibly allege that identity theft could be perpetrated using his  
23 name and address, particularly given such information likely is publicly available.

24 Likewise, Plaintiff cannot manufacture damages by claiming “he was forced to  
25 purchase credit monitoring services and undertake other efforts to reduce the risk of  
26 identity theft from the security breach.” Compl. ¶ 93. As a matter of law, the “future  
27 harm being mitigated” must be “imminent.” *In re Adobe Sys., Inc. Privacy Litig.*, 66  
28 F. Supp. 3d 1197, 1217 (N.D. Cal. 2014); *see also Ables v. Brooks Bros. Grp.*, 2018

1 WL 8806667, at \*7 (C.D. Cal. June 7, 2018) (“In the absence of increased risk of  
2 future harm, neither time nor money expended by Ables to mitigate a hypothetical risk  
3 confers standing.”); *Beck v. McDonald*, 848 F.3d 262, 276 (4th Cir. 2017) (plaintiffs’  
4 allegations “that they wish to enroll in, are enrolled in, or have purchased credit  
5 monitoring services ... do not constitute an injury in fact”). As shown below, Plaintiff  
6 fails entirely to establish a plausible risk of imminent future harm.

7 In the end, from a monetary standpoint, Plaintiff has failed to plead an  
8 actionable loss by virtue of the Alleged Breach. And Plaintiff’s remaining alleged  
9 “harms” fare no better:

10 Alleged non-notification. Even if the Alleged Breach occurred (and it did not),  
11 Plaintiff fails to plead facts showing he suffered an injury *as a result of any alleged*  
12 *failure to notify* him of the nonexistent breach. *In re Sony Gaming Networks &*  
13 *Customer Data Sec. Breach Litig.*, 996 F. Supp. 2d 942, 1010 (S.D. Cal. 2014)  
14 (plaintiff “must allege actual damages flowing from the unreasonable delay (and not  
15 just the intrusion itself) in order to recover actual damages”). To the contrary,  
16 Plaintiff admits he has not suffered “identity theft” or “theft of property.” Compl. ¶  
17 85. Nor does Plaintiff claim the alleged non-notification prevented him from taking  
18 allegedly necessary prophylactic steps. *Id.* ¶ 8.

19 Alleged overpayment. Plaintiff claims “[o]verpayments to [Walmart] for the  
20 goods bought from [Walmart], as it was understood that a portion of that price would  
21 be applied to the costs of implementing reasonable and adequate safeguards and  
22 security measures that would protect their PII, which [Walmart] failed to implement.”  
23 Compl. ¶ 42(g). But courts have squarely rejected that theory, stating it is “cognizable  
24 only where a consumer purchases defective or falsely advertised products, or—in the  
25 data breach context—in the presence of a security agreement concerning consumer  
26 data or some other representation that the cost of security is subsumed within the cost  
27 of goods.” *Ables*, 2018 WL 8806667, at \*7. Plaintiff fails to allege any representation  
28 that the “cost of security is subsumed within the cost of goods” he allegedly bought



1 from Walmart. Indeed, Plaintiff fails to allege any facts showing the goods he  
2 allegedly bought online were more expensive than those sold in a brick-and-mortar  
3 Walmart store—the natural consequence of paying an additional premium for  
4 information security.

5 To the extent Plaintiff relies on Walmart’s Privacy Policy, such reliance is  
6 misplaced. Compl. ¶ 97. Walmart’s Terms of Use (“TOU”) specifically warn  
7 customers that “ANY INFORMATION YOU SEND OR RECEIVE DURING YOUR  
8 USE OF THE WALMART SITES MAY NOT BE SECURE AND MAY BE  
9 INTERCEPTED OR OTHERWISE ACCESSED BY UNAUTHORIZED PARTIES.”  
10 RJN, Exh. G.<sup>4</sup> “Courts have held that similar language is sufficient to put consumers  
11 on notice that a company’s data security practices are not bulletproof,” thereby  
12 defeating alleged benefit of the bargain damages. *Jackson v. Loews Hotels, Inc.*, 2019  
13 WL 6721637, at \*2 (C.D. Cal. July 24, 2019) (rejecting similar overpayment theory in  
14 data breach action). Accordingly, Plaintiff’s benefit of the bargain theory fails.

15 Diminished value of PII. Plaintiff claims “[a]scertainable losses in the form of  
16 deprivation of the value of [his] PII.” Compl. ¶ 42(e). As courts have held, however,  
17 “absent any allegation that [Plaintiff] want[s] to sell [his] financial information to  
18 someone else, deprivation of value is not a cognizable form of injury.” *Smith v. Sabre*  
19 *Corp.*, No. 17-cv-5149, at 6 n.3 (C.D. Cal. Jan. 23, 2018) (ECF No. 36) (citing *Khan*  
20 *v. Children’s Nat’l Health Sys.*, 188 F. Supp. 3d 524, 533 (D. Md. 2016)). Plaintiff  
21 makes no such allegation here, and his “lost PII value” theory should be rejected.  
22

---

23  
24 <sup>4</sup> Courts across the country have taken judicial notice of web pages available through  
25 the Wayback Machine. *See, e.g., Erickson v. Neb. Mach. Co.*, 2015 WL 4089849, at  
26 \*1 (N.D. Cal. July 6, 2015) (“Courts have taken judicial notice of the contents of web  
27 pages available through the Wayback Machine as facts that can be accurately and  
28 readily determined from sources whose accuracy cannot reasonable be questioned...  
and the Court does so here.”); *In re Facebook, Inc. Sec. Litig.*, 405 F. Supp. 3d 809,  
829 (N.D. Cal. 2019) (taking judicial notice of prior iterations of Facebook’s data  
policy via the Wayback Machine).

1        Imminent and certainly impending future harm. Plaintiff’s own admissions  
 2 doom his claim of alleged future harm. He admits “closing or modifying financial  
 3 accounts” as a result of the Alleged Breach. Compl. ¶ 41. As courts have held in  
 4 connection with that same allegation, Plaintiff eliminated any risk of future harm  
 5 relating to those accounts. *Jackson v. Loews Hotels, Inc.*, 2019 WL 2619656, at \*3  
 6 (C.D. Cal. Jan. 4, 2019) (“Plaintiff’s allegations also foreclose the possibility of a  
 7 certainly impending future harm regarding the exposure of her financial information.  
 8 She alleges that after the data breach she ‘clos[ed] or modif[ied]’ her ‘financial’  
 9 accounts.”); *Ables*, 2018 WL 8806667, at \*5 (“Once Ables cancelled those disclosed  
 10 credit and debit card accounts, those account ‘number[s], expiration date[s], and  
 11 security code[s] were rendered useless,’ and the fact that his full name was made  
 12 publicly available does not plausibly give rise to a current need for credit  
 13 monitoring.”) (citing *Engl v. Nat. Grocers by Vitamin Cottage, Inc.*, 2016 WL  
 14 8578252, at \*6 (D. Colo. Sept. 21, 2016)); *Sabre Corp.*, No. 17-cv-5149, at 4 n.2  
 15 (ECF No. 36) (“[T]he fact that Smith admitted that she cancelled her cards was fatal to  
 16 her claims because it meant that there could be no future risk to those accounts and  
 17 nothing to ‘constantly monitor’ them for.”) (citing *Whalen v. Michaels Stores, Inc.*,  
 18 2017 WL 1556116, at \*2 (2d Cir. May 2, 2017)).

19        Even if Plaintiff had not “clos[ed] or modif[ied]” the accounts allegedly  
 20 impacted by the Alleged Breach (as he admits he did), he still cannot show a  
 21 legitimate risk of future harm stemming from the alleged compromise of his payment  
 22 card information. “[G]iven the zero-fraud-liability policy of every major card issuer  
 23 in the country,” Plaintiff would face no risk of liability for fraudulent charges.  
 24 *Whalen v. Michaels Stores Inc.*, 153 F. Supp. 3d 577, 581 (E.D.N.Y. 2015).

25        There is no risk of future harm based on the alleged compromise of Plaintiff’s  
 26 remaining information—*i.e.*, name and address. Compl. ¶ 3. Plaintiff does not and  
 27 cannot show how identify theft could be committed using only his name and address,  
 28 which is fatal. *See Provost v. Aptos, Inc.*, 2018 WL 1465766, at \*5 (N.D. Ga. Mar.



12, 2018); *see also* *Ables*, 2018 WL 8806667, at \*5 (“[A]s described above, cancellation of the compromised credit and debit card accounts extinguished any concrete risk of future identity theft, and the FAC fails to explain how the wrongdoers’ possession of Ables’ first and last name exposes him to such a substantial risk.”). Plaintiff cannot show an imminent risk of future harm.

In the end, Plaintiff has not and cannot plead the requisite damages and injury elements of his negligence, unfair competition, or contract claims.

### C. Plaintiff’s Claims Fail for Additional Reasons

#### 1. Plaintiff’s Negligence Claim Fails (Count II)

Because Plaintiff does not allege “physical harm (*i.e.*, personal injury or property damage),” the “economic loss doctrine” bars his negligence claim “as a matter of law.” *In re Sony Gaming Networks & Customer Data Sec. Breach Litig.*, 903 F. Supp. 2d 942, 959-61 (S.D. Cal. 2012). Plaintiff’s alleged damages (Compl. ¶ 85) fall squarely within the rule. *Castillo v. Seagate Tech., LLC*, 2016 WL 9280242, at \*5 (N.D. Cal. Sept. 14, 2016) (“Economic losses include damages for inadequate value, costs of repair, loss of expected proceeds, loss of use, loss of goodwill, and damages paid to third parties.”). Plaintiff’s failure to allege any personal injury or property damage is dispositive. The economic loss rule applies and bars his negligence claim.

#### 2. Plaintiff’s Unfair Competition Claim Fails (Count III)

Plaintiff cannot show he lacks adequate legal remedies: Just this year, the Ninth Circuit held that a plaintiff cannot pursue equitable remedies under the UCL—*e.g.*, restitution, injunctive relief—unless he can establish he lacks an adequate remedy at law. *Sonner v. Premier Nutrition Corp.*, 971 F.3d 834, 845 (9th Cir. 2020) (affirming dismissal of UCL claim where the plaintiff “fail[ed] to demonstrate that she lacks an adequate legal remedy”). Numerous courts have dismissed UCL claims in the wake of *Sonner* for that very reason. *See, e.g., In re Macbook Keyboard Litig.*, 2020 WL 6047253, at \*4 (N.D. Cal. Oct. 13, 2020); *Gibson v. Jaguar Land Rover N.*

1 *Am., LLC*, 2020 WL 5492990, at \*3 (C.D. Cal. Sept. 9, 2020); *Schertz v. Ford Motor*  
 2 *Co.*, 2020 WL 5919731, at \*2 (C.D. Cal. July 27, 2020); *Adams v. Cole Haan, LLC*,  
 3 2020 WL 5648605, at \*2 (C.D. Cal. Sept. 3, 2020) (“The clear rule in *Sonner* [is] that  
 4 plaintiffs must plead the inadequacy of legal remedies before requesting equitable  
 5 relief[.]”).

6 Here, Plaintiff has not pled an inadequate legal remedy. In fact, Plaintiff claims  
 7 he “has suffered compensable damages.” Compl. ¶ 7. Thus, his own allegations  
 8 foreclose the possibility that a legal remedy would be inadequate. Moreover,  
 9 Plaintiff’s UCL claim “relies on the same factual predicates as [his] legal causes of  
 10 action,” all of which seek money damages in connection with the Alleged Breach.  
 11 *Madrigal v. Hint, Inc.*, 2017 WL 6940534, at \*4-5 (C.D. Cal. Dec. 14, 2017)  
 12 (quotation and citation omitted) (dismissing UCL and unjust enrichment claims  
 13 because they rely on the same factual predicates as plaintiff’s legal claims); *see*  
 14 *Fonseca v. Goya Foods, Inc.*, 2016 WL 4698942, at \*7 (N.D. Cal. Sept. 8, 2016).  
 15 Plaintiff’s UCL claim should be dismissed.

16 Plaintiff lacks statutory standing: In any event, Plaintiff lacks statutory  
 17 standing to bring a UCL claim because he cannot show he lost money or property as a  
 18 result of the Alleged Breach. Cal. Bus. & Prof. Code § 17204; *see also Dugas v.*  
 19 *Starwood Hotels & Resorts Worldwide, Inc.*, 2016 WL 6523428, at \*11 (S.D. Cal.  
 20 Nov. 3, 2016) (“In order to establish standing under the UCL, a plaintiff’s claim must  
 21 specifically involve lost money or property.”).

22 *First*, Plaintiff cannot claim he lost money or property based on any alleged  
 23 monetary expenditures. As stated above, Plaintiff does not allege any fraudulent  
 24 charges were made using his payment card information. Similarly, Plaintiff cannot  
 25 claim he lost money as a result of any credit monitoring expenditures—that is a non-  
 26 cognizable self-inflicted “harm,” given the lack of any real imminent risk of future  
 27 harm. Likewise, Plaintiff cannot show “overpayments.” Plaintiff has not and cannot  
 28 show he paid more money for a particularized measure or form of data security.

1        *Second*, Plaintiff cannot claim he lost money or property based on his flawed  
 2 lost PII value theory. As a matter of law, “‘personal information’ does not constitute  
 3 money or property under the UCL.” *In re iPhone Application Litig.*, 2011 WL  
 4 4403963, at \*14 (N.D. Cal. Sept. 20, 2011); *see also In re Facebook Privacy Litig.*,  
 5 791 F. Supp. 2d 705, 714 (N.D. Cal. 2011) (“[P]ersonal information does not  
 6 constitute property for purposes of a UCL claim.”); *In re Google Inc. St. View Elec.*  
 7 *Commc’ns Litig.*, 794 F. Supp. 2d 1067, 1086 (N.D. Cal. 2011) (“A plaintiff’s  
 8 ‘personal information’ does not constitute property under the UCL.”).

9        *Third*, Plaintiff cannot claim he lost money or property based on any allegedly  
 10 imminent risk of future harm. Even if such risk existed (and it does not), allegations  
 11 of future harm do not suffice. *In re Sony*, 903 F. Supp. 2d at 966 (“Plaintiffs’  
 12 allegations that the heightened risk of identity theft, time and money spent on  
 13 mitigation of that risk, and property value in one’s information, do not suffice as  
 14 injury under the UCL, FAL, and/or the CLRA.”); *Dugas*, 2016 WL 6523428, at \*11  
 15 (plaintiff’s claim that “he will incur damages to monitor identity theft, and that he has  
 16 spent time responding to the unauthorized charges on his credit card” was insufficient  
 17 to establish UCL standing). Plaintiff’s inability to show “lost money or property” is  
 18 fatal to his UCL claim, and it should be dismissed on that basis alone.

19        Plaintiff cannot predicate his UCL claim on alleged violations of other laws:

20        Plaintiff bases his UCL claim on alleged violations of the CCPA, CRA, and  
 21 FTC Act. Plaintiff, however, cannot do so.

22        The CCPA: The CCPA expressly prohibits Plaintiff from predicating his UCL  
 23 claim on an alleged violation of the CCPA. On its face, the CCPA states that “nothing  
 24 in this title shall be interpreted to serve as the basis for a private right of action under  
 25 any other law,” such as the UCL. Cal. Civ. Code § 1798.150(c).

26        In this respect, Walmart need only show “another provision [] actually ‘bar[s]’  
 27 the action.” *Rose v. Bank of Am., N.A.*, 57 Cal. 4th 390, 398 (2013) (quoting *Cel-Tech*  
 28 *Commc’ns, Inc. v. Los Angeles Cellular Tel. Co.*, 20 Cal. 4th 163, 183 (1999)). And

Section 1798.150(c) does just that. As the California Senate Judiciary Committee acknowledged before the CCPA’s passage, Section 1798.150(c) “eliminates the ability of consumers to bring claims for violations of the Act under statutes such as the [UCL].” Sen. Judiciary Committee Report, June 26, 2018, p. 22; September 12, 2019 California Senate Rules Committee Report on 2019 CA A.B. 1355 (Section 1798.150 is the “only enforcement mechanism made available to consumers pursuant to the CCPA”). On top of that, as explained in Section V(A), Plaintiff has not adequately pled a CCPA violation.

The CRA: As explained in Section A, Plaintiff has not shown the Alleged Breach involved actionable “personal information” under the CRA.

The FTC Act: Plaintiff’s vague and conclusory references to the FTC Act fall short of the mark. Plaintiff must “plead with particularity how the facts of this case pertain to that specific statute.” *Baba v. Hewlett-Packard Co.*, 2010 WL 2486353, at \*6 (N.D. Cal. June 16, 2010). Plaintiff cannot do so.

Plaintiff claims “[c]onsumers cannot avoid the injury themselves because they are not informed of the severe vulnerabilities presented by the website.” Compl. ¶ 92. As stated above, however, Plaintiff suffered no injury. Moreover, Walmart informed customers that “ANY INFORMATION YOU SEND OR RECEIVE DURING YOUR USE OF THE WALMART SITES MAY NOT BE SECURE AND MAY BE INTERCEPTED OR OTHERWISE ACCESSED BY UNAUTHORIZED PARTIES.”

### 3. Plaintiff’s Contract Theories Fail (Counts IV-VI)

Walmart’s TOU expressly bars Plaintiff’s contract claims. In the “Disclaimer of Warranties” in Section 17, Plaintiff agreed to “ASSUME FULL RESPONSIBILITY FOR [HIS] USE OF THE WALMART SITES AND AGREE[D] THAT ANY INFORMATION [HE] SEN[T] OR RECEIVE[D] DURING [HIS] USE OF THE WALMART SITES **MAY NOT BE SECURE AND MAY BE INTERCEPTED OR OTHERWISE ACCESSED BY UNAUTHORIZED PARTIES.**” RJN, Exh. G (TOU) § 17 (emphasis added). Plaintiff further agreed that

1 “NO WALMART ENTITY IS RESPONSIBLE FOR ANY LOSS OR DAMAGE TO  
2 [HIS] PROPERTY OR DATA THAT RESULTS FROM ANY MATERIALS YOU  
3 ACCESS OR DOWNLOAD FROM THE WALMART SITES.” *Id.*

4 Moreover, in the “Limitation of Liability” in Section 18, Plaintiff agreed that,  
5 “TO THE FULLEST EXTENT PROVIDED BY APPLICABLE LAW, WALMART  
6 ENTITIES WILL NOT BE LIABLE TO [HIM] OR TO ANY OTHER PERSON  
7 UNDER ANY CIRCUMSTANCES OR UNDER ANY LEGAL OR EQUITABLE  
8 THEORY, WHETHER IN TORT, CONTRACT, STRICT LIABILITY, OR  
9 OTHERWISE, FOR ANY INDIRECT, SPECIAL, INCIDENTAL, OR  
10 CONSEQUENTIAL LOSSES OR DAMAGES OF ANY NATURE EVEN IF AN  
11 AUTHORIZED REPRESENTATIVE OF A WALMART ENTITY HAS BEEN  
12 ADVISED OF OR SHOULD HAVE KNOWN OF THE POSSIBILITY OF SUCH  
13 DAMAGES.” RJN Exh. G (TOU) § 18. Plaintiff agreed that disclaimer “APPLIES  
14 TO, BUT IS NOT LIMITED TO, ANY DAMAGES OR INJURY ARISING FROM  
15 ANY FAILURE OF PERFORMANCE, ERROR, OMISSION, INTERRUPTION,  
16 DELETION, DEFECTS, DELAY IN OPERATION OR TRANSMISSION, LOST  
17 PROFITS, LOSS OF GOODWILL, LOSS OF DATA, WORK STOPPAGE,  
18 ACCURACY OF RESULTS, COMPUTER FAILURE OR MALFUNCTION,  
19 COMPUTER VIRUSES, FILE CORRUPTION, COMMUNICATION FAILURE,  
20 NETWORK OR SYSTEM OUTAGE, **THEFT, DESTRUCTION,**  
21 **UNAUTHORIZED ACCESS TO, ALTERATION OF, LOSS OF USE OF ANY**  
22 **RECORD OR DATA, AND ANY OTHER TANGIBLE OR INTANGIBLE LOSS.”**  
23 *Id.* (emphasis added).

24 “With respect to claims for breach of contract, limitation of liability clauses are  
25 enforceable unless they are unconscionable, that is, the improper result of unequal  
26 bargaining power or contrary to public policy.” *Food Safety Net Servs. v. Eco Safe*  
27 *Sys. USA, Inc.*, 209 Cal. App. 4th 1118 (2012). And Plaintiff pleads no such facts  
28 here. Nor could he. Limitation-of-liability clauses “have long been recognized as

valid in California,” and courts routinely enforce them where, as here, third-party conduct is involved. *See, e.g., Caraccioli v. Facebook, Inc.*, 167 F. Supp. 3d 1056, 1063 (N.D. Cal. 2016) (enforcing limitation-of-liability clause that applied to claims arising out of third-party conduct); *Food Safety*, 209 Cal. App. 4th at 1126. The TOU’s limitation-of-liability provision is enforceable, and it should be enforced. Each of Plaintiff’s contract claims fails thereunder.<sup>5</sup>

## **VI. CONCLUSION**

For these reasons, the Court should dismiss Plaintiff’s complaint in its entirety. Because the stated defects are irremediable, the dismissal should be with prejudice.

Dated: December 14, 2020

**HUNTON ANDREWS KURTH LLP**

By: /s/ Ann Marie Mortimer

Ann Marie Mortimer

Jason J. Kim

Jeff R. R. Nelson

Attorneys for Defendant

WALMART INC.

<sup>5</sup> Even under the version of the TOU to which Plaintiff admitted his assent in opposition to Walmart’s motion to compel arbitration, Plaintiff agreed Walmart would not be liable for “ANY INDIRECT, SPECIAL, INCIDENTAL OR CONSEQUENTIAL LOSSES OR DAMAGES OF ANY NATURE ARISING OUT OF OR IN CONNECTION WITH THE USE OF OR INABILITY TO USE THE WALMART SITES, INCLUDING, WITHOUT LIMITATION, DAMAGES FOR LOST PROFITS, LOSS OF GOODWILL, LOSS OF DATA, WORK STOPPAGE, ACCURACY OF RESULTS, OR COMPUTER FAILURE OR MALFUNCTION.” ECF No. 27-1, Exhs. 1 & 2.